The University of Kansas

INFORMATION
& TELECOMMUNICATION
TECHNOLOGY CENTER
The University of Kansas

Technical Report

Final Report
Rail Sensor Testbed Program: Active Agents in Containers for Transport Chain Security

Gary J. Minden, Victor S. Frost, Joseph B. Evans,
Jun Huan, Leon S. Searl, Dan DePardo,
Ed Komp, Ruoyi Jiang, Martin Kuehnhausen

ITTC-FY2011-TR-47750-11

March 21, 2011

Project Sponsor:
Office of Naval Research
Contract: N00014-07-1-1042
The University of Kansas

1 REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YY)*
21-03-2011

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
25-06-2007 – 31-12-2010

4. TITLE AND SUBTITLE

Final Report-Rail Sensor Testbed Program:
Active Agents in Containers for Transport Chain Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER
N00014-07-1-1042

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Gary J. Minden, Victor S. Frost, Joseph B. Evans, Jun Huan, Leon S. Searl, Dan DePardo, Ed Komp, Ruoyi Jiang, Martin Kuehnhausen

5d. PROJECT NUMBER
07PR07594-00

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The University of Kansas Center for Research, Inc.
Information and Telecommunications
Technology Center
2385 Irving Hill Road
Lawrence, KS 66045

8. PERFORMING ORGANIZATION REPORT NUMBER
TR ITTC-FY2011-TR-47750-11

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Naval Research Laboratory
ATTN: ONR-BD253
875 North Randolph Street
Arlington, Va. 22203-1995

10. SPONSORING/MONITORING AGENCY ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT Research was conducted on making transported objects (e.g., containers, pallets, and boxes) active participants in their own security. This effort focused on improving transportation security by enabling the objects being transported to become active agents in their own protection. Here, the objects are equipped with sensing and communication capabilities and are able to determine and communicate their sense of security throughout the dynamic transportation chain in a distributed manner. As part of the project, we have developed several data mining algorithms to enable intelligent agents to detect changes from their environment state. We have also designed algorithms to allow agents to communicate with each other for enhancing safety for the group of agents. Research issues of the designed algorithms have been applied to the Transportation Security SensorNet(TSSN) real transportation chain. We have tested all the new algorithms on real sensor data collected from transportation sensor network environments. The results have demonstrated the effectiveness of these algorithms for wireless sensor network security applications and provided useful insights regarding the challenges of the anomaly detection problem for distributed security in challenging environments. In addition the "lessons learned" from our experiments are documented and a set of requirements for possible future systems were formulated.

15. SUBJECT TERMS
Sensor Network, Transportation Security, Anomaly Localization, Regularization, Joint Sparsity, Transfer learning, large margin classifier, transductive learning, L1 Regularization, Graph Classification, Semi-Structured Data

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT:**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** (Monitor) Tommy R. Albrecht
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	SAR		**19b. TELEPHONE NUMBER** *(Include Area Code)* 703-696-8732

Abstract

Research was conducted on making transported objects (e.g., containers, pallets, and boxes) active participants in their own security. This effort focused on improving transportation security by enabling the objects being transported to become active agents in their own protection. Here, the objects are equipped with sensing and communication capabilities and are able to determine and communicate their sense of security throughout the dynamic transportation chain in a distributed manner. As part of the project, we have developed several data mining algorithms to enable intelligent agents to detect changes from their environment state. We have also designed algorithms to allow agents to communicate with each other for enhancing safety for the group of agents. Research issues of the designed algorithms have been applied to the Transportation Security SensorNet (TSSN) real transportation chain. We have tested all the new algorithms on real sensor data collected from transportation sensor network environments. The results have demonstrated the effectiveness of these algorithms for wireless sensor network security applications and provided useful insights regarding the challenges of the anomaly detection problem for distributed security in challenging environments. In addition the "lessons learned" from our experiments are documented and a set of requirements for possible future systems were formulated.

Table of Contents

Section **Page**

List of Figures

Final Report-
Rail Sensor Testbed Program:
Active Agents in Containers for Transport Chain Security

1 Introduction

The goal of this effort was to improve rail security over trade lanes, e.g., transport from Mexico to an inland port at Kansas City. This effort focused on transporter identification, sensing, real-time monitoring and tracking, safety and compliance, and integration of local, state, and federal information. We focused on transiting from the current centralized model to a distributed one. The distributed model is based on making transported objects (e.g., containers, pallets, and boxes) *active agents in their own security*. The effort leveraged the application of effective container sealing using advanced RFID technologies, sensing, application of new radio technologies, and information management. Evaluation prototypes were built and deployed and new distributed sensor algorithms were developed.

Section 2 outlines the approach to the project. Section 3 describes the research tasks and Section 4 lists published papers and personnel who worked on the project.

There are two appendices. Appendix A describes the algorithms used by the agents to detect anomalous events and experiments. Details and analyses of the algorithms are in the published papers (see Section 4). Appendix B captures "lessons learned" from our experiments and is a set of requirements for possible future systems.

2 Project Overview

Current approaches to providing security of the container transport chain are based on a hierarchical approach in terms of the collection and analysis of critical information. In all current approaches the objects being transported are passive, that is, they are simply labeled, possibly with an RFID tag (there are exceptions for some perishable items that include simple temperature sensors). The information in the label can be extensive, but is static.

The actual container transport chain is highly *distributed*, involving complex processes, since there is no single system governing the international movement of containers. For example, the security function is distributed among industries, regulatory agencies, liability regimes and legal frameworks. Such a distributed system is not represented well by the current hierarchical approaches to security. In addition, the state of the containers being transported is *dynamic*. For example, the location, movement, temperature, means of transportation, and even access limitations of a container change from the time it is loaded until it is unloaded at its final destination.

As the cost of sensors, computing, and communications continues to decrease there is an opportunity to fundamentally change the centralized security model and move to a distributed one, which better represents the current reality. The distributed model is based on making transported objects (e.g., containers, pallets, and boxes) *active agents in their own security*. In the distributed model each object is monitored by a set of embedded sensors and intelligent agents. An agent continuously senses its environment, the state of its object, and the state of neighboring objects. Each agent has a description of what constitutes a "secure" state. If the agent determines that the object has left the current notion of a "secure" state then a decision is required to determine whether the new state is one where the object's safety is violated or whether the change is an acceptable deviation.

As an example, consider the transport of bags of money, where each bag includes an accelerometer, a processor executing the agent program, and a radio. The bags are loaded onto a truck and the agents communicate their accelerometer readings to each other; as long as all the readings are (reasonably) consistent, the agents have a degree of confidence that they are traveling together. However, if one bag observes significantly different readings (indicating that the bag is moving in a different direction or at a different speed from the others, meaning that it is probably off the truck), then there maybe a problem which needs to be communicated (based on [2]). In this simple example the agents define a "safe" state and conditions that violate that state. The presence of two-way communications and processing provides the opportunity to enable more complex monitoring behaviors.

Our work transformed the problem from an external, periphery base model to an integrated, distributed model where agents dynamically work together and develop as a team to achieve greater security. The distributed model is that of endowing physical objects with the ability to determine and communicate their sense of security through consistency of information combined with sensor observations of their environment.

The following research questions were addressed

1. How are "object security states described?" What are the semantics and ontology to describe and reason about object security states?
2. How do distributed agents form an initial mutually consistent security state? How do distributed agents maintain a mutually consistent security state?
3. How does an agent detect a change from the mutually consistent security state?
4. How does an agent determine if a detected change is permissible? How does an agent update its perspective of consistency?
5. How can trade data exchange (centralized) information be used to as part of the consistency model?
6. How does the distributed model scale (a) with number of elements, (b) with the number of objects, (c) processing time and energy, (d) communications, (e) number of sensors, and (f) number of agents?
7. What are the deployment costs and utility tradeoffs?

2.1 Rail SensorNet Architecture

In this section we describe the Rail SensorNet architecture for monitoring trusted corridors and how the distributed approach is integrated into this architecture.

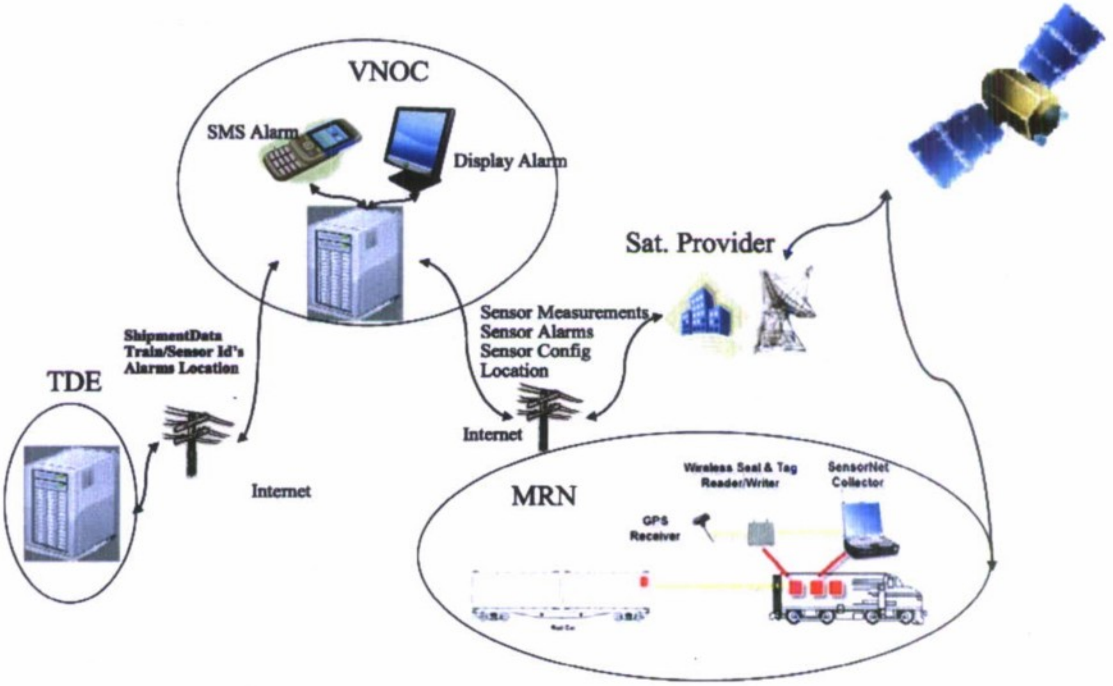

Figure 1 System Architecture of the Rail SensorNet

The Rail SensorNet is comprised of the following components:

1. A Mobile Rail Network (MRN). The MRN includes sensors on containers and cargo, a control processor in the locomotive, a GPS receiver, and one or more communications devices (e.g., cellular telephone and satellite telephone).
2. One or more communications networks, e.g., cellular telephone network, satellite network, and/or Internet.
3. A Virtual Network Operating Center (VNOC).
4. A Trade Data Exchange (TDE).

The MRN includes sensors on containers and cargo, a control processor in the locomotive, a GPS receiver, and one or more communications devices (e.g., cellular telephone and satellite telephone). The distributed agent system communicates events to the MRN control processor.

The communications networks in the Rail SensorNet are commercial services. Events are transmitted from the MRN to the VNOC and control messages transmitted from the VNOC to the MRN over the communications networks.

The VNOC includes a database storing data about the cargo in transit, event filtering functions, and notification services. The VNOC filters events. For example, a "Sensor Seal Open Event" when the geographical location is a known freight yard is OK. But, the same event outside the freight yard would cause an alert. Alerts are sent to responsible parties based on attributes of the cargo. An alert for a container containing hazardous material might be sent to emergency services while an alert on low value cargo might only be sent to the railroad operator. Alerts are sent via thc cellular short message service, email, or Internet services.

The concept of a Trade Data Exchange is described in [4]. The TDE:

1. Captures commercial clearance data, including Shipping List, Bill of Lading, Commercial Invoice, Certificate of Origin (NAFTA Letter), and Shippers Export Declaration.
2. Interconnects commercial, regulatory and security stakeholders.
3. Validates and verifies data to ensure accuracy, consistency and completeness.
4. Performs forward notification to thc customs broker to request verification of the trade origination documents. The customs broker accesses the TDE via the same portal to review and verify the trade documentation.
5. Monitors the progress of the documentation via the TDE and notifies responsiblc parties when errors or incompleteness pose the threat of delaying a shipment.
6. Performs risk assessment.

The applications running on the MRN, VNOC, and TDE communicate using Service Oriented Architecture (SOA) protocols. Thus, it is relatively easy to extend the system with new services.

2.2 Agent Based Systems

There are many definitions of an "intelligent agent" (or simply, "agent"), but most researchers agree that an agent is an *autonomous* program that has the ability to *sense* thc environment, the ability to *communicate* with users and other agents, and the ability to *effect changes* to the environment. Additionally, agents may be able to *learn* new behaviors, *collaborate* with others to resolve conflicts or perform tasks, and *negotiate* to share limited resources.

Agent technology fits well in the proposed research since the software entities tracking the security state of a physical object, e.g., a container, need to operate continuously without human supervision (autonomously), must sense the state of the world, and must be able to communicate amongst each other and possibly to other systcm components. In this context agents must be able to sound alarms or perform actions that change the environment. In our model agents can also learn different definitions of "security," thus expanding their knowledge. The ability to learn is essential, since it is improbable that the developers of the agents can foresee and pre-program all expected states of the world. Consequently, the agents will need the ability to expand their notion of what is a safe and what is an insecure state. Such learning requires the ability of the agents to collaborate and negotiate with others to resolve potential concerns.

Consider two example scenarios. Assume that the initial state of "safety" for a container is defined as "no change from current state." Let us also assume that the train on which a container is placed starts to move, changing the container's location and velocity. This change in the current state would make the container agent assume it is now in a potentially unsafe state, and would lead it to query the agents around it if they thought they, too, were unsafe. A "super-agent" which has the appropriate credentials informs the container agent that the current state change is appropriate and the new state is still safe. Given that the "super-agent" has the authority to define safe and unsafe states, the container agent accepts that. The agent learns that after being loaded on a train it expects a change in location and velocity.

In the second example, the exact scenario as above is considered, but now there is no super-agent. In this case the other container agents on the train verify that they are also experiencing the same change, indicating they are all moving together. This information is compared to stored transport schedule information. If the timing of the motion is consistent with the transport schedule then the objects return to a safe state.

The approach builds upon related work on reputation systems and the web of trust approach to security. The web of trust approach (popularized by PGP in the information security community) involves the use of data (signatures) from multiple trusted sources to allow redundant verification of the veracity of the data. Reputation systems [12, 13] utilize information from multiple sources to provide a decentralized mechanism for establishing the veracity of the sources of information. These trust approaches have been applied to a variety of regimes, including virtual communities [14], email [15] and ecommerce [16] and [17], and sensor networks [18]. These approaches define trust between players and develop associated trust models; frameworks for reputation systems exist. The "sense of security" concepts we developed have similarities with trust. The paradigm required a technical definition of "sense of security" and development of associated models similar to [14]. Transport security requires a highly agile architecture to adapt to the inherently dynamic environment and an architecture that can embed this capability in relatively inexpensive, low-power computing and communications resources.

The new paradigm also has similarities to autonomic computing [19] where "systems manage themselves according to high-level behavioral specifications" [20]. Autonomic computing is currently targeted toward automating large computing systems like data centers. The general operation of autonomic computing involves an autonomic manager that executes a monitor-analyze-plan-execute loop that is targeted to achieve behavioral outcome, commonly system performance (e.g., maximum throughput) optimization [20].

3 Research Tasks

The research project was organized into the following tasks.

3.1 Model Development

We identified the basic research issues associated with the proposed new paradigm. An ontology was defined, that is, the meaning of consistency and ways of establishing a mutually consistent view between distributed objects. An ontology is: the objects, concepts, and other entities that are assumed to exist in some area of interest and the relationships that hold among them [22]. For agent systems that are considered here, what "exists" is that which can be represented. When the knowledge of a domain is represented in a declarative formalism, the set of objects that can be represented is called the universe of discourse. Pragmatically, an ontology defines the vocabulary with which queries and assertions are exchanged among agents. Ontological commitments are agreements to use the shared vocabulary in a coherent and consistent manner. The agents sharing a vocabulary need not share a knowledge base, each knows things the other does not, and an agent that commits to an ontology is not required to answer all queries that can be formulated in the shared vocabulary.

We defined an ontology in the context of Transport Chain Security. Distributed algorithms enabling objects to detect a change from their consistent state were developed as part of this task and are described in Appendix A. Such changes occur as the object is transported in a normal situation, thus the object's perspective of consistency is dynamic.

The result of this task is the architecture for a system where physical objects are endowed with the ability to determine and communicate their sense of security through consistency of information combined with sensor observations of their environment.

3.2 Mapping to Enabling Technologies

In this task we mapped our distributed paradigm onto specific technologies. To test the architecture several use cases for a rail sensor testbed will be developed. From these use cases one or more prototypes will be designed and implemented, building upon the ongoing effort to develop SensorNet technologies to monitor trusted corridors. The result of this task will be a prototype design and implementation for physical objects endowed with the ability to determine and communicate their sense of security through consistency of information combined with sensor observations of their environment.

3.3 Prototype Development and Logistics

Testbeds and field prototypes are valuable for gaining an understanding of the real-world system trade-offs and identifying practical barriers to ubiquitous use of the technology. We executed a number of experiments to collect data for testing our implementations. Results of these experiments are reported in Appendix A and published papers.

3.4 Prototype Deployment and Evaluation

We deployed a prototype in the Rail SensorNet environment. Data and experiences collected during a number of trials are reported in Appendix B as a set of requirements for a future Rail SensorNet.

4 Results

4.1 Reports and Technical Papers

The following technical reports and published papers resulted from work on this project.

[1] Q. Brian, et al., "Anomaly Detection with Sensor Data for Distributed Security," in ICCCN '09: Proceedings of the 2009 Proceedings of 18th International Conference on Computer Communications and Networks, ed: IEEE Computer Society, 2009, pp. 1-6.

[2] H. Fei and J. Huan, "L2 norm regularized feature kernel regression for graph data," in Proceeding of the 18th ACM conference on Information and knowledge management, ed. Hong Kong, China: ACM, 2009, pp. 593-600.

[3] H. Fei and J. Huan, "Boosting with structure information in the functional space: an application to graph classification," in Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining, ed. Washington, DC, USA, 2010, pp. 643-652.

[4] H. Fei, et al., "GLSVM: Integrating Structured Feature Selection and Large Margin Classification," in ICDM Workshops, ed, 2009, pp. 362-367.

[5] R. Jiang, et al., "Anomaly Localization by Joint Sparse PCA and Its Implementation in Sensor Network.," in Sensor KDD, ed, 2010.

[6] B. Quanz and J. Huan, "Aligned Graph Classification with Regularized Logistic Regression," in Proc. 2009 SIAM International Conference on Data Mining, ed, 2009.

[7] B. Quanz and C. Tsatsoulis, "Determining Object Safety using a Multiagent, Collaborative System," in Environment-Mediated Coordination in Self-Organizing and Self-Adaptive Systems (ECOSOA 2008) Workshop, ed. Venice, Italy, 2008.

4.2 Personnel

The project supported the following faculty in EECS: V. Frost, G. Minden, J. Evans, J. Huan, and C. Tsatsoulis.

The project also supported Mr. Leon Searl, Mr. Dan DePardo, and Mr. Dan Deavours members of our technical staff.

The following graduate students worked on the project: R. Jiang, B. Quanz, H. Fei, M. Kuehnhausen, D. Fokum, and M. Zeets.

The following students worked on the project as undergraduates: A Oguna.

5 References

1. Kanoun, O. and H.-R. Tränkler, *Sensor technology advances and future trends.* IEEE Transactions on Instrumentation and Measurement, 2004. **53**(6): p. 1497-1501.
2. David G. Simmons. *Project Sun Small Programmable Object Technology Sun SPOTs,.* in *Based on Net-Ready Sensors: The Way Forward, Oak Ridge National Laboratory*. 2006.
3. *Container Transport Security Across Modes.* Organization for Economic Co-Operation And Development, European Conference of Ministers of Transport, 2005.
4. Dean Kothmann. *From Shelf to Shelf – Continuous Cargo Visibility and Integrity.* in *Innovation World Conference, Kansas City, Missouri*. 2006.
5. Soh, L.-K. and C. Tsatsoulis, *A Real-Time Negotiation Model and a Multi-Agent Sensor Network Implementation.* Autonomous Agents and Multi-Agent Systems, 2005. **11**(3): p. 215-271.
6. Soh, L.-K. and C. Tsatsoulis. *Utility-Based Multiagent Coalition Formation with Incomplete Information and Time Constraints.* in *IEEE International Conference on Systems, Man, and Cybernetics*. 2003.
7. Soh, L.-K. and C. Tsatsoulis, *Learning to Form Negotiation Coalitions in a Multiagent System.* AAAI Spring Symposium on Collaborative Learning Agents 2002: p. 106-12.
8. Soh, L.-K. and C. Tsatsoulis. *Reflective Negotiating Agents for Real-Time Multisensor Target Tracking.* in *Int. J. Conf. On Artificial Intelligence (IJCAI-01), Seattle, WA* 2001.
9. Soh, L.-K. and C. Tsatsoulis. *Agent-Based Argumentative Negotiations with Case-Based Reasoning* in *AAAI Fall Symposium on Negotiation Methods for Autonomous Cooperative Systems*. 2001.
10. Soh, L.-K., C. Tsatsoulis, and H. Sevay, *A Satisficing, Negotiated, and Learning Coalition Formation Architecture*, in *Distributed Sensor Networks: A Multiagent Perspective*, C. Ortiz, V. Lesser and M. Tambe Editor. 2003, Kluwer. p. 109-138.
11. Sevay, H. and C. Tsatsoulis, *Agent-Based Intelligent Information Dissemination in Dynamically Changing Environments, in: Intelligent Agents and their Applications*, in *Studies in Fuzziness and Soft Computing*, L.C. Jain, Z. Chen, and N. Ichalkaranje, Editor. 2002, Physica-Verlag. p. 1-26.
12. Resnick, P., et al., *Reputation systems.* Commun. ACM, 2000. **43**(12): p. 45-48.
13. Abdul-Rahman, A., *A framework for decentralised trust reasoning*, in *Ph.D. dissertation, University College London*. 2005.
14. Abdul-Rahman, A. and S. Hailes. *Supporting trust in virtual communities.* in *Proceedings of the 33rd Hawaii International Conference on System Sciences. Maui, HW.* 2000.
15. Boykin, P.O. and V. Roychowdhury, *Personal email networks: an effective anti-spam tool.* 2004(http://www.arxiv.org/abs/cond-mat/0402143).
16. Melnik, M., Alm, J., *Does a seller's eCommerce reputation matter? evidence from eBay auctions.* . J. Journ. of Indust. Econ., 2002. **50**(3): p. 337-349.

17. Tran, T. and R. Cohen. *Improving User Satisfaction in Agent-Based Electronic Market-places by Reputation Modeling and Adjustable Product Quality.* in *Proc. of the Third Int. Joint Conf. on Autonomous Agents and Multi Agent Systems (AAMAS-04)*. 2004.

18. Ganeriwal, S., Srivastava, M. B. . *Reputation-based framework for high integrity sensor networks.* in *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington DC, USA, October 25 - 25, 2004*. 2004.

19. Menasce, D.A. and J.O. Kephart, *Guest Editors' Introduction: Autonomic Computing.* Internet Computing, 2007. **11**(1): p. 18-21.

20. Tesauro, G., *Reinforcement Learning in Autonomic Computing: A Manifesto and Case Studies.* Internet Computing, 2007. **11**(1): p. 18-21.

21. Cybenko, G. and V. Berk, *Process Query Systems.* IEEE Computer, 2007. **40**(1): p. 62-70.

22. Genesereth, M. and N. Nilsson, *Logical Foundations of Artificial Intelligence. .* 1987, Stanford: Morgan Kaufmann.

Appendix A

Rail Sensor Testbed Program: Active Agent in Containers for Transport Chain Security: Algorithms